Forensic Hardware and Sofware
0384
Report Produced : 12/04/2019 11:57:52
Produced By : [redacted]

Forensic Hardware and Sofware
0384
Report Produced : 12/04/2019 11:57:52
Produced By : [redacted]

Case Details

Case Reference	0384
IDMS Reference	2019-010614
Examiner	[redacted]
Case Service Level	PRIORITY
Analysis Type	Job Performance Failure
Case Classification Level	UNCLASSIFIED
Service Level	7 Days
Open Date/Time	08/13/2019 08:10:46 (-0400)
Due Date/Time	08/20/2019 23:59:59 (-0400)
Case Status	Open
Contact Name	[redacted]
Assigned Staff Member Name	[redacted]
Record Status	Unlocked
Case Background	2 Desktop Computers submitted on 8/13/19; 2 additional desktop computers submitting on 8/21/19.
Background Attachment(s)	2019-010614 Request Form.pdf Leonard Notes.docx

Technical Review

Technical Review	Yes
Appropriate examinations have been performed to address request	Yes
Report is clear and understandable	Yes
The procedures performed were adequately documented and forensically sound	Yes
Exam documentation was sufficiently detailed to enable reproduction of the results	Yes

The interpretations and conclusions of the examiner were reasonable	Yes
Report is consistent with the examination documentation	Yes
When generally accepted examination tools are not used, are significant findings verified by the examiner?	Yes
Results media has been spot checked	Yes
Examiner performing review	ITS Canabal
Date of review	09/11/2019

Contact Details

First Name	[redacted]
Last Name	[redacted]
Sector	New York Field Office
Primary Email	[redacted]
Authority Contact Name	[redacted]
Authority Contact Number	7034131860
Authority Contact Email	[redacted]
Authority Status	Approved

Case Assets

Product Name	Tableau TD2
Asset Tag	X29946
Case Process	Evidence Imaging - Write Blocker (0002)
Tracked Asset	Yes
Asset Type	Hardware
Product Name	Tableau TD2
Asset Tag	X29946
Case Process	Evidence Imaging - Write Blocker (0004)
Tracked Asset	Yes
Asset Type	Hardware
Product Name	Alienware
Asset Tag	X29717
Case Process	Unknown
Tracked Asset	Yes
Asset Type	Hardware
Product Name	Aegis Fortress
Asset Tag	101300010379
Case Process	Unknown
Tracked Asset	Yes
Asset Type	Hardware

Case Collection

Collection Date/Time	08/11/2019 11:28:00 (-0400)
Collection From	[redacted]
Collection Type	Collection
Method	Staff Collection

Evidence Status	Complete
Assigned Staff Member Name	[redacted]
Office	Cyber Investigations Office New York
Company	US Department of Justice Office of the Inspector General
CompanyAddress	1401 S Clark St. Suite 900 Arlington VA 22202 United States
Company Contact Name	Cyber Investigations Washington
Company Contact Number	[redacted]

Collected Exhibits

Evidence Reference	0001
Evidence Type	Desktop
Seal Number	N/A
Description	HP EliteDesk 800 S/N: 2UA4381YNJ
Evidence Reference	0002
Evidence Type	Hard Drive
Seal Number	N/A
Description	Seagate 500 GB SATA HDD S/N: Z6E8M349
Evidence Reference	0003
Evidence Type	Desktop
Seal Number	N/A
Description	HP EliteDesk 800 S/N: 2UA4381YMW
Evidence Reference	0004
Evidence Type	Hard Drive
Seal Number	N/A
Description	Seagate 500 GB SATA HDD S/N: Z6E8K1EV
Attachment(s)	ECD In.pdf
Collection Date/Time	08/21/2019 00:00:00 (-0400)
Collection From	[redacted] [redacted]
Collection Type	Collection
Method	Staff Collection
Evidence Status	Complete
Assigned Staff Member Name	[redacted]
Office	New York Field Office
Company	US Department of Justice Office of the Inspector General
CompanyAddress	1 Battery Park Plaza 29th Floor New York New York 10004 United States

Company Contact Name	New York Field Office

Collected Exhibits

Evidence Reference	0005
Evidence Type	Desktop
Seal Number	N/A
Description	HP EliteDesk 800 S/N: 2UA4381XJW
Evidence Reference	0006
Evidence Type	Hard Drive
Seal Number	N/A
Description	Seagate 500GB SATA HDD S/N: Z6E8KD3N
Evidence Reference	0007
Evidence Type	Desktop
Seal Number	N/A
Description	HP Compaq 8200 Elite
Evidence Reference	0008
Evidence Type	Hard Drive
Seal Number	N/A
Description	Hitachi 500GB SATA HDD S/N: JP1572JE36LSNK
Attachment(s)	ECD in.pdf

Evidence Details

Evidence Reference	0001
Evidence Type	Desktop
Logged In Date/Time	08/11/2019 04:15:35 (-0400)
Original Seal Number	N/A
Storage Location	Washington Vault
Priority	High
Description	HP EliteDesk 800 S/N: 2UA4381YNJ
Property Number	0214 207268
Seized Date/Time	08/11/2019 11:00:34 (-0400)
Seized By/Produced By	[redacted]
Processing Result	N/A
Archived	No

Pre-Imaging Details

Start Date/Time	08/14/2019 19:15:45 (-0400)
End Date/Time	08/14/2019 19:25:00 (-0400)
Conducted By (Name)	[redacted]
Manufacturer	Hewlett Packard
Model	EliteDesk 800
Serial Number	2UA381YNJ
Casing Type	Workstation
Casing Colour	Black
BIOS Key	F10
BIOS Date/Time	08/14/2019 19:21

Actual Date/Time	08/14/2019 19:21
Password Protected	No
Attachment(s)	IMG_0075.JPG
Evidence Reference	0002
Evidence Type	Hard Drive
Logged In Date/Time	08/11/2019 04:15:35 (-0400)
Original Seal Number	N/A
Storage Location	Washington Vault
Priority	High
Description	Seagate 500 GB SATA HDD S/N: Z6E8M349
Property Number	N/A
Seized Date/Time	08/11/2019 11:00:30 (-0400)
Seized By/Produced By	[redacted]
Processing Result	N/A
Archived	No
Attachment(s)	Hash Match.jpg
Pre-Imaging Details	
Start Date/Time	08/11/2019 16:00:00(-0400)
Conducted By (Name)	[redacted]
Manufacturer	Seagate
Model	ST500DM002
Serial Number	Z6E8M349
Type	SATA HDD
Notes	Drive removed from desktop 0214 207268 for imaging by Lidsky on 8/11/19 at CC lab.
Attachment(s)	
Imaging Details	
Start Date/Time	08/11/2019 16:40:28 (-0400)
End Date/Time	08/11/2019 18:14:00 (-0400)
Conducted By (Name)	[redacted]
Software Used	Tableau
Write Blocker	Tableau TD2 (X29946)
Image Type	E01
Compression	None
Block Size	64
Cyclic Redundancy Check (CRC)	64
MD5	13e7ad6132719bae78d849e3fb914cc2
SHA1	465c7bf5f62aebb6c98ecfc60534110f56274c25
Image Verified	No
Imaging Workstation	N/A
Notes	Imaging cancelled by Lidsky prior to verification completion. Subsequent hash match confirmed (see info under evidence details). Imaging started: 2019-08-11 16:43 Imaging finished: 2019-08-11 18:14

Tableau device serial number: 11d2003b
Tableau firmware revision: 4.01
Tableau firmware timestamp: May 02 2013 21:35:47
Source device model: ST500DM002-1BD142
Source device serial number: Z6E8M349
Source device HPA in use: No
Source device DCO in use: No
Source device capacity reported Pwr-ON: 976,773,168 (500.1 GB)
Source device capacity reported by HPA: 976,773,168 (500.1 GB)
Source device capacity reported by DCO: 976,773,168 (500.1 GB)

Attachment(s)	2019-08-11 16-43-11 00107 D2F.LOG
Evidence Reference	0003
Evidence Type	Desktop
Logged In Date/Time	08/13/2019 09:00:35 (-0400)
Original Seal Number	N/A
Storage Location	Washington Vault
Priority	High
Description	HP EliteDesk 800 S/N: 2UA4381YMW
Property Number	0214 207270
Seized Date/Time	08/11/2019 11:00:03 (-0400)
Seized By/Produced By	[redacted]
Processing Result	N/A
Archived	No
Pre-Imaging Details	
Start Date/Time	08/14/2019 19:00:00 (-0400)
End Date/Time	08/14/2019 19:25:00 (-0400)
Conducted By (Name)	[redacted]
Manufacturer	Hewlett Packard
Model	EliteDesk 800
Serial Number	2UA4381YMW
Casing Type	Workstation
Casing Colour	Black
BIOS Key	F10
BIOS Date/Time	08/14/2019 19:18
Actual Date/Time	08/14/2019 19:18
Password Protected	No
Attachment(s)	IMG_0073.JPG
Evidence Reference	0004
Evidence Type	Hard Drive
Logged In Date/Time	08/13/2019 09:00:35 (-0400)
Original Seal Number	N/A
Storage Location	Washington Vault
Priority	High
Description	Seagate 500 GB SATA HDD S/N: Z6E8K1EV

Property Number	N/A
Seized Date/Time	08/11/2019 11:00:01 (-0400)
Seized By/Produced By	[redacted]
Processing Result	N/A
Archived	No

Pre-Imaging Details

Start Date/Time	08/11/2019 16:00:00(-0400)
Conducted By (Name)	[redacted]
Manufacturer	Seagate
Model	ST500DM002
Serial Number	Z6E8K1EV
Type	SATA HDD
Notes	Drive removed from desktop 0214 207270 for imaging by Lidsky on 8/11/19 at CC lab.

Attachment(s)

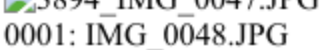
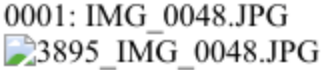
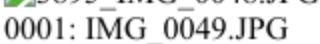
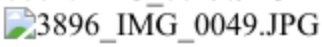
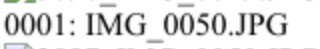
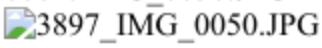
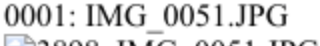
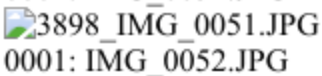
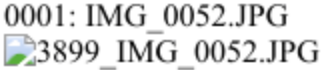
Imaging Details

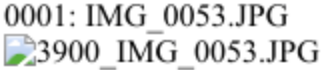
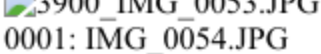
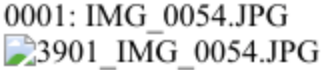
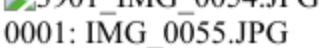
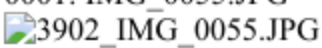
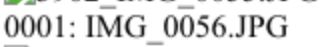
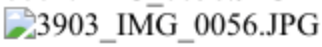
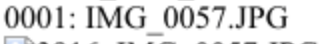
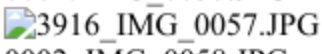
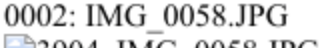
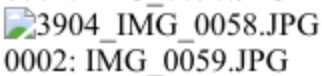
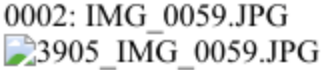
Start Date/Time	08/11/2019 18:17:11 (-0400)
End Date/Time	08/11/2019 21:16:00 (-0400)
Conducted By (Name)	[redacted]
Software Used	Tableau
Write Blocker	Tableau TD2 (X29946)
Image Type	E01
Compression	None
Block Size	64
Cyclic Redundancy Check (CRC)	64
MD5	48f956e5ddab702d48177534ec96d026
SHA1	be9791bce5978ccdf3111a54eac84606739c0424
Image Verified	No
Imaging Workstation	N/A

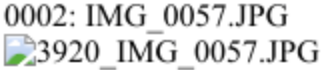
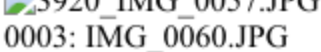
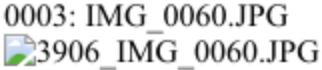
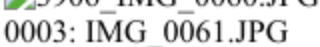
Notes	Imaging started: 2019-08-11 18:17 Imaging finished: 2019-08-11 21:16 Tableau device serial number: 11d2003b Tableau firmware revision: 4.01 Tableau firmware timestamp: May 02 2013 21:35:47 Source device model: ST500DM002-1BD142 Source device serial number: Z6E8K1EV Source device HPA in use: No Source device DCO in use: No Source device capacity reported Pwr-ON: 976,773,168 (500.1 GB) Source device capacity reported by HPA: 976,773,168 (500.1 GB) Source device capacity reported by DCO: 976,773,168 (500.1 GB)
Attachment(s)	2019-08-11 18-17-23 00108 D2F.LOG

Case Photographs

0001: IMG_0046.JPG
3893_IMG_0046.JPG

0001: IMG_0047.JPG

3894_IMG_0047.JPG
0001: IMG_0048.JPG

3895_IMG_0048.JPG
0001: IMG_0049.JPG

3896_IMG_0049.JPG
0001: IMG_0050.JPG

3897_IMG_0050.JPG
0001: IMG_0051.JPG

3898_IMG_0051.JPG
0001: IMG_0052.JPG

3899_IMG_0052.JPG
0001: IMG_0053.JPG

3900_IMG_0053.JPG
0001: IMG_0054.JPG

3901_IMG_0054.JPG
0001: IMG_0055.JPG

3902_IMG_0055.JPG
0001: IMG_0056.JPG

3903_IMG_0056.JPG
0001: IMG_0057.JPG

3916_IMG_0057.JPG
0002: IMG_0058.JPG

3904_IMG_0058.JPG
0002: IMG_0059.JPG

3905_IMG_0059.JPG
0002: IMG_0057.JPG

3920_IMG_0057.JPG
0003: IMG_0060.JPG

3906_IMG_0060.JPG
0003: IMG_0061.JPG

3907_IMG_0061.JPG
0003: IMG_0062.JPG

3908_IMG_0062.JPG
0003: IMG_0063.JPG

3909_IMG_0063.JPG
0003: IMG_0064.JPG

3910_IMG_0064.JPG
0003: IMG_0065.JPG

3911_IMG_0065.JPG
0003: IMG_0066.JPG

3912_IMG_0066.JPG
0003: IMG_0067.JPG

3913_IMG_0067.JPG
0003: IMG_0068.JPG

3914_IMG_0068.JPG
0003: IMG_0069.JPG

3915_IMG_0069.JPG
0004: IMG_0069.JPG

3917_IMG_0069.JPG
0004: IMG_0070.JPG

3918_IMG_0070.JPG
0004: IMG_0071.JPG

3919_IMG_0071.JPG

Case Disposal